(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-229091
(P2004-229091A)
(43)公開日　平成16年8月12日(2004.8.12)

(51)Int.Cl.[7]	F I		テーマコード（参考）
H04L 12/56	H04L 12/56	100A	5K030
H04L 12/46	H04L 12/46	E	5K033
	H04L 12/46	100R	

審査請求 有　請求項の数 15　OL　（全 20 頁）

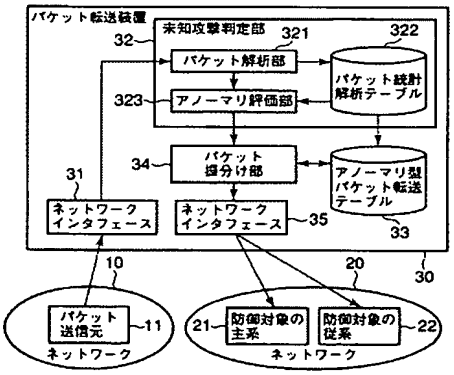
(21)出願番号　特願2003-16290 (P2003-16290)
(22)出願日　平成15年1月24日 (2003.1.24)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(74)代理人　100058479
弁理士　鈴江　武彦
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100084618
弁理士　村松　貞男
(74)代理人　100092196
弁理士　橋本　良郎

最終頁に続く

(54)【発明の名称】パケット転送システム、パケット転送装置、プログラム及びパケット転送方法

(57)【要約】
【課題】攻撃検知の正確性が完全でない場合でも、防御対象の正常なサービスを停止させず、防御対象の致命的な被害から守ることにある。
【解決手段】同一のサービス機能をもつ主系２１及び従系２２を備えた冗長構成の防御対象とし、かつ、防御対象にパケットを転送するパケット転送装置３０は、防御対象の冗長化構成テーブル３３を設け、パケット送信元１１から防御対象をアクセスする通信アプリケーションデータを解析し、統計的な評価から攻撃可能性を判定したとき、防御対象の冗長構成を参照し、受信パケットを従系に転送することにより、パケットが攻撃性でないとき、主系とほぼ同様のサービス機能を提供することができる。一方、従系が受け取ったパケットが真に攻撃的なパケットであれば、直接の被害を受けるが、その被害は従系であり、主系は直接の被害を受けなくなるから、未知の攻撃に対して、防御対象の可用性が高い。
【選択図】　図１



【特許請求の範囲】
【請求項１】
主系及び従系を備えた冗長構成化された防御対象と、
パケット送信元からネットワークを通じて前記防御対象をアクセスするパケットを受信し、この受信されたパケットに関するアプリケーションデータを解析し、統計的な評価のもとに攻撃の可能性を判定し、攻撃可能性の有無に応じて該当受信パケットを前記防御対象の主系と従系とに振分け転送するパケット転送装置とを備えたことを特徴とするパケット転送システム。
【請求項２】
請求項１に記載のパケット転送システムにおいて、
前記防御対象の従系は、前記主系とほぼ同じサービス提供機能を有し、前記攻撃の可能性有りとして受け取ったパケットが真の攻撃でなかった場合には前記主系に代わってサービスを提供することを特徴とするパケット転送システム。
【請求項３】
パケット送信元からネットワークを通じて防御対象をアクセスするパケットを受信し、冗長構成化された主系と従系に振分け転送するパケット転送装置であって、
前記受信パケットに関するアプリケーションデータを解析し、統計的な評価のもとに未知の攻撃の可能性有無を判定する未知攻撃判定手段と、
前記防御対象のネットワークの冗長構成を規定する手段と、
前記未知攻撃判定手段による攻撃可能性有無の判定結果と前記冗長構成とに基づき、前記受信パケットを前記主系と従系とに振分け転送するパケット振分け手段と
を備えたことを特徴とするパケット転送装置。
【請求項４】
主系及び従系を有する防御対象のネットワークの冗長構成が記憶され、パケット送信元からネットワークを通じて防御対象をアクセスするパケットを受信し、同一のサービス提供機能をもつ防御対象の主系と従系に振分け処理するコンピュータに、
前記受信パケットの内容を解析し、統計的な評価に基づく統計情報を取得するパケット解析機能と、この解析機能によって取得された統計情報から攻撃可能性の有無を判定するアノーマリ評価機能と、この評価機能の判定結果を受け、前記記憶された冗長構成を参照し、パケット転送先を振分け決定する転送先決定機能と、この決定機能による転送先決定に基づいて前記受信パケットを前記主系又は前記従系に転送するパケット転送機能とを実現させることを特徴とするプログラム。
【請求項５】
パケット送信元からネットワークを通じて防御対象をアクセスするパケットを受信するパケット受信ステップと、
この受信パケットに関するアプリケーションデータを解析し、統計的な評価に基づく統計情報を取得するパケット解析ステップと、
この統計情報から攻撃可能性の有無を判断するアリーマリ評価ステップと、
このステップによる攻撃可能性の有無に応じて前記防御対象を構成するほぼ同一機能をもつ主系と従系との何れかの振分けを決定するパケット振分けステップと、
この振分けに従って前記受信パケットを前記主系又は前記従系に転送するパケット転送ステップを有することを特徴とするパケット転送方法。
【請求項６】
ホスト型ＩＤＳをもつ主系及び複数のホスト型ＩＤＳをもつ従系を備えた冗長構成化された防御対象と、
パケット送信元からネットワークを通じて前記防御対象をアクセスするパケットを受信し、この受信されたパケットに関するアプリケーションデータを解析し、統計的な評価のもとに攻撃の可能性を判定し、攻撃可能性の有無に応じて該当受信パケットを前記防御対象の主系と従系とに振分け転送し、転送先の前記ホスト型ＩＤＳをもつ従系側から攻撃検知の通知を受けた場合、次の受信パケットを次のホスト型ＩＤＳをもつ従系に切替えて転送

可能とするパケット転送装置とを備えたことを特徴とするパケット転送システム。
【請求項７】
主系及びホスト型ＩＤＳをもつ複数の従系を備えた冗長構成化された防御対象と、
パケット送信元からネットワークを通じて前記防御対象をアクセスするパケットを受信し、この受信されたパケットに関するアプリケーションデータを解析し、統計的な評価のもとに攻撃の可能性を判定し、攻撃可能性有りの場合に統計的に異常な複数の値域又は前記アプリケーションデータの変数名に従って前記受信パケットを所定のホスト型ＩＤＳをもつ従系に転送するパケット転送装置とを備えたことを特徴とするパケット転送システム。
【請求項８】
パケット送信元からネットワークを通じて防御対象をアクセスするパケットを受信し、冗長構成化された主系とホスト型ＩＤＳをもつ複数の従系の何れか１つに振分け転送するパケット転送装置であって、
前記受信パケットに関するアプリケーションデータを解析し、統計的な評価のもとに未知の攻撃の可能性有無を判定する未知攻撃判定手段と、
前記防御対象のネットワークの冗長構成を規定する手段と、
前記未知攻撃判定手段によって攻撃可能性有りの判定結果と前記冗長構成とに基づき、前記受信パケットを所定の従系に振分け転送するパケット振分け手段と、
このパケット転送後、転送先のホスト型ＩＤＳをもつ従系側から攻撃検知の通知を受けた場合、転送先従系側が攻撃検知したと認識する従系攻撃検知識別手段と、
この識別手段によって攻撃検知と認識した場合、前記受信パケットを前記冗長構成に従って次の従系に切替えて転送する従系切替手段と
を備えたことを特徴とするパケット転送装置。
【請求項９】
パケット送信元からネットワークを通じて防御対象をアクセスするパケットを受信し、冗長構成化された主系とホスト型ＩＤＳをもつ複数の従系の何れか１つに振分け転送するパケット転送装置であって、
前記受信パケットに関するアプリケーションデータを解析し、統計的な評価のもとに未知の攻撃の可能性有無を判定する未知攻撃判定手段と、
前記防御対象のネットワークの冗長構成を規定する手段と、
前記未知攻撃判定手段によって攻撃可能性有りの判定結果の場合、この判定結果による統計的に異常な複数の値域又は前記アプリケーションデータの変数名に従って前記受信パケットを所定のホスト型ＩＤＳをもつ従系に転送するパケット振分け手段と
を備えたことを特徴とするパケット転送装置。
【請求項１０】
主系及びホスト型ＩＤＳをもつ複数の従系を有する防御対象のネットワークの冗長構成が記憶され、パケット送信元からネットワークを通じて防御対象をアクセスするパケットを受信し、同一のサービス提供機能をもつ防御対象の主系と従系に振分け処理するコンピュータに、
前記受信パケットの内容を解析し、統計的な評価に基づく統計情報を取得するパケット解析機能と、この解析機能によって取得された統計情報から攻撃可能性の有無を判定するアノーマリ評価機能と、この評価機能に攻撃可能性有りの判定結果を受け、前記記憶された冗長構成を参照し、何れか１つのホスト型ＩＤＳをもつ複数の従系をパケット転送先として決定する転送先決定機能と、この決定機能による転送先決定に基づいて前記受信パケットを前記従系に転送するパケット転送機能と、パケット転送後、転送先のホスト型ＩＤＳをもつ従系側から攻撃検知の通知を受けた場合、転送先従系側が攻撃検知したと認識する従系攻撃検知識別機能と、攻撃検知と認識した場合、受信パケットを前記冗長構成に従って次の従系に切替えて転送する従系切替機能と
を備えたことを特徴とするパケット転送装置。
【請求項１１】
パケット送信元からネットワークを通じて防御対象をアクセスするパケットを受信するパ

ケット受信ステップと、
この受信パケットに関するアプリケーションデータを解析し、統計的な評価に基づく統計情報を取得するパケット解析ステップと、
この統計情報から攻撃可能性の有無を判定するアリーマリ評価ステップと、
このステップによる攻撃可能性有りの場合、所定の１つの従系に振分けを決定するパケット振分けステップと、
この振分けに従って前記受信パケットを前記所定の１つの従系に転送するパケット転送ステップと、
パケット転送後、転送先のホスト型ＩＤＳをもつ従系側から攻撃検知の通知を受けた場合、転送先従系側が攻撃検知したと認識する従系攻撃検知識別ステップと、
攻撃検知と認識した場合、前記冗長構成に従って次の従系に切替える従系切替ステップとを有することを特徴とするパケット転送方法。

【請求項１２】
請求項８に記載のパケット転送装置において、
前記従系攻撃検知識別手段によって攻撃検知と認識した場合、該当アプリケーションデータをアノーマリ評価関数により再評価し、その評価値を閾値とし、統計的に特に異常な値域に組み込むことを特徴とするパケット転送装置。

【請求項１３】
主系及び少なくとも１つの従系を備えた冗長構成化された防御対象と、
パケット送信元から送られてくるパケットに関するアプリケーションデータを解析し、統計的な評価のもとに攻撃の可能性を判定し、攻撃可能性の有無に応じて前記パケットを前記防御対象の主系と従系とに振分け転送する複数のパケット転送装置と、
ＵＲＬと転送先との関係を規定する負荷分散テーブルが設けられ、前記パケット送信元から送られてくるパケットに関するアプリケーションデータに含まれるＵＲＬを解読し、当該負荷分散テーブルに規定される前記複数のパケット転送装置及び前記防御対象の何れか１つに受信パケットを送信する負荷分散装置と
を備えたことを特徴とするパケット転送システム。

【請求項１４】
請求項１３に記載するパケット転送システムにおいて、
前記負荷分散装置の負荷分散テーブルに規定するＵＲＬと転送先との関係は、変数の有無、変数の数によって定めるものであるパケット転送システム。

【請求項１５】
主系及び少なくとも１つの従系を備えた冗長構成化された防御対象が設けられ、パケットを当該主系及び前記１つの従系に分散転送するパケット転送方法において、
パケットに関するアプリケーションデータに含まれるＵＲＬと転送先との関係が規定され、パケット送信元から送られてくるパケットに関するアプリケーションデータを解読し、この解読結果から得られるＵＲＬに基づき、前記複数のパケット転送装置及び前記防御対象の何れか１つに受信パケットを送信する負荷分散ステップを有し、
この負荷分散ステップのもとにパケットを受信した各パケット転送装置が前記請求項５又は請求項１１の一連の処理を実行することを特徴とするパケット転送方法。

【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、ネットワークに対する不正侵入検知技術等に利用されるパケット転送システム、パケット転送装置、プログラム及びパケット転送方法に関する。

【０００２】
【従来の技術】
従来、Ｗｅｂサーバやメールサーバへの不正侵入を早期に検知するために、幾つかの不正侵入検知技術（ＩＤＳ：Ｉｎｔｒｕｓｉｏｎ　Ｄｅｔｅｃｔｉｏｎ　Ｓｙｓｔｅｍ）が考えられている。

【０００３】
その１つは、複数のパケットから得られるアプリケーションデータの統計的解析により、未知の攻撃の可能性を検知する技術が挙げられる。未知の攻撃とは、攻撃の手法が知られておらず、予め記述可能なアプリケーションデータの文字パターンでは検知できない攻撃をいう。
【０００４】
この統計的解析を用いた不正侵入検知技術は、図１３に示すように防御対象にアクセスしようとするパケットを受信した後、これら複数のパケットから得られるアプリケーションデータの統計的な解析を行い、正常であるか異常であるかを統計的に評価する技術である。この解析によって評価値が統計的に異常な値域に属する場合は攻撃の可能性有りと判定し、警報を発したり、受信パケットを遮断するなどの処置がとられている。
【０００５】
他の１つは、不正侵入監視部を備えた正規サーバ及び通信セッション引継部を備えたおとりサーバとを設け、不正侵入監視部は、正規サーバと外部端末との間に確立された通信セションに基づき、パスワードの設定時に間違え回数が基準値を越えた場合、或いはポートスキャンのアクセスを実行した場合、外部端末からの不正侵入と判定し、その不正侵入と判定された通信セションをおとりサーバの通信セッション引継部に引き継がせることにより、正規サーバを防御する不正侵入検知システムである。
【０００６】
【特許文献１】
特開２００２－１１１７２７号公報（図２）
【０００７】
【発明が解決しようとする課題】
しかしながら、前者の不正侵入検知技術は、アプリケーションデータの統計的解析結果から攻撃の可能性を判定する技術であり、確実に攻撃するとは確定できない未確定の状態にある。その結果、実際には攻撃でないにも拘らず攻撃と誤検知する可能性がある。仮に誤検知した場合にはパケットを遮断してしまうことから、正常なサービスが提供できなくなる。一方、真の攻撃であった場合、パケットを遮断せずに取込むことから、警報を発するが、防御対象が致命的な被害を受けてしまう。
【０００８】
一方、後者の不正侵入検知システムは、意図的にセキュリティ性を脆弱させたいわゆるハニーポットと称するおとりサーバを設け、これを正規のサーバのように見せかけて攻撃をおびき寄せ、攻撃に関する情報を収集するものである。しかし、ハニーポット自体には本来のサービスを提供する機能が備わっておらず、また未知の攻撃の場合には真の攻撃であるか否かが不確実な状態にあるので、前述同様に攻撃でないにも拘らず攻撃と誤検知しおとりサーバに振分けてしまうと、防御対象の正常なサービスを提供できなくなってしまう。
本発明は上記事情にかんがみてなされたもので、未知の攻撃に対し、確実な攻撃検知の判定が難しい状態でも、防御対象の正常なサービスを停止させず、かつ、防御対象の致命的な被害から守るパケット転送システム、パケット転送装置、プログラム及びパケット転送方法を提供することを目的とする。
【０００９】
【課題を解決するための手段】
上記課題を解決するために、本発明に係わるパケット転送システムは、主系及び従系を備えた冗長構成化された防御対象と、パケット送信元からネットワークを通じて前記防御対象をアクセスするパケットを受信し、この受信されたパケットに関するアプリケーションデータを解析し、統計的な評価のもとに攻撃の可能性を判定し、攻撃可能性の有無に応じて該当採取パケットを前記防御対象の主系と従系とに振分け転送するパケット転送装置とを設けた構成である。
【００１０】

この発明は以上のような構成とすることにより、統計的な評価のもとに攻撃の可能性が判定されれば、主系と同様のサービス提供機能をもつ従系に振り分けるので、攻撃で無い場合にはサービスを提供することが可能になる。攻撃を受けた場合には、従系であるので、防御対象の主系は致命的な被害を受けることがない。

【００１１】

（２）　本発明は、パケット送信元からネットワークを通じて防御対象をアクセスするパケットを受信し、冗長構成化された主系と従系に振分け転送するパケット転送装置であって、

前記受信パケットに関するアプリケーションデータを解析し、統計的な評価のもとに未知の攻撃の可能性有無を判定する未知攻撃判定手段と、前記防御対象のネットワークの冗長構成を規定する手段と、未知攻撃判定手段による攻撃可能性有無の判定結果と冗長構成とに基づき、受信パケットを主系と従系とに振分け転送するパケット振分け手段とを設けたパケット転送装置である。

【００１２】

この発明においては、受信パケットに関するアプリケーションデータの統計的な解析により評価し、未知の攻撃の可能性があれば、ネットワークの冗長構成から従系に振り分けるので、前記（１）と同様の作用効果を奏する。

【００１３】

なお、プログラム及び所定の処理手順に基づく方法によっても以上のような一連の処理を実現することが可能である。

【００１４】

（３）　本発明に係るパケット転送システムは、ホスト型ＩＤＳをもつ主系及び複数のホスト型ＩＤＳをもつ従系を備えた冗長構成化された防御対象と、パケット送信元からネットワークを通じて前記防御対象をアクセスするパケットを受信し、この受信されたパケットに関するアプリケーションデータを解析し、統計的な評価のもとに攻撃の可能性を判定し、攻撃可能性の有無に応じて該当受信パケットを前記防御対象の主系と従系とに振分け転送し、転送先の前記ホスト型ＩＤＳをもつ従系側から攻撃検知の通知を受けた場合、次のホスト型ＩＤＳをもつ従系に切替えてパケットを転送可能とするパケット転送装置とを設けた構成であるので、前記（１）と同様の作用効果を奏する他、従系側から攻撃検知の通知を受けた場合に次の従系に振り分けるので、攻撃を受けた従系を復旧される間でも、次の従系によりサービスを提供することが可能である。

【００１５】

なお、従系間の振分けについては、攻撃可能性有りの場合に統計的に異常な複数の値域又はアプリケーションデータの変数名に従って振り分けてもよい。

【００１６】

（４）　本発明は、パケット送信元からネットワークを通じて防御対象をアクセスするパケットを受信し、冗長構成化された主系とホスト型ＩＤＳをもつ複数の従系の何れか１つに振分け転送するパケット転送装置であって、

前記受信パケットに関するアプリケーションデータを解析し、統計的な評価のもとに未知の攻撃の可能性有無を判定する未知攻撃判定手段と、前記防御対象のネットワークの冗長構成を規定する手段と、前記未知攻撃判定手段によって攻撃可能性有りの判定結果と前記冗長構成とに基づき、前記受信したパケットを所定の従系に振分け転送するパケット振分け手段と、このパケット転送後、転送先のホスト型ＩＤＳをもつ従系側から攻撃検知の通知を受けた場合、転送先従系側が攻撃検知したと認識する従系攻撃検知識別手段と、この識別手段によって攻撃検知と認識した場合、前記冗長構成に従って次の従系に切替えて受信パケットを転送可能とする従系切替手段とを設けた構成である。

【００１７】

この発明においても、前記（３）と同様な作用効果を奏することができる。

【００１８】

なお、プログラム及び所定の処理手順に基づく方法によっても以上のような一連の処理を

実現することが可能である。

【００１９】

（５）　本発明に係るパケット転送システムは、主系及び少なくとも１つの従系を備えた冗長構成化された防御対象と、パケット送信元から送られてくるパケットに関するアプリケーションデータを解析し、統計的な評価のもとに攻撃の可能性を判定し、攻撃可能性の有無に応じて前記パケットを前記防御対象の主系と従系とに振分け転送する複数のパケット転送装置と、ＵＲＬと転送先との関係を規定する負荷分散テーブルが設けられ、前記パケット送信元から送られてくるパケットに関するアプリケーションデータに含まれるＵＲＬを解読し、当該負荷分散テーブルに規定される前記複数のパケット転送装置及び前記防御対象の何れか１つに受信パケットを送信する負荷分散装置とを設けた構成である。

【００２０】

この発明においては、前記（１）と同様の作用効果を奏する他、負荷分散によりスループットの低下を抑制できる。

【００２１】

【発明の実施の形態】

以下、本発明の実施の形態について図面を参照して説明する。

【００２２】

（第１の実施の形態）

図１は本発明に係るパケット転送システム及びパケット転送装置の一実施の形態を示す構成図である。

【００２３】

このパケット転送システムは、インターネットなどの第１のネットワーク１０とインターネット、専用ライン、ＬＡＮその他の伝送ラインなどで構成される第２のネットワーク２０と、これらネットワーク１０，２０間を行き来するパケットを受け取って転送するパケット転送装置３０とによって構成されている。

【００２４】

第１のネットワーク１０は、未知の攻撃を仕掛けると想定される例えばクライアント端末などを含むパケット送信元１１が設けられている。パケット送信元１１は、未知の攻撃を仕掛けるか否かを無視すれば、図示されていないが複数存在することは言うまでもない。

【００２５】

一方、第２のネットワーク２０は、主系２１と従系２２よりなる防御対象が設けられ、防御対象のいわゆる冗長化構成が採用されている。この防御対象としては、例えばＷｅｂサーバやＦＴＰ（Ｆｉｌｅ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ）サーバなどであり、主系２１は正しいグループのパケットを受け取るサーバであり、従系２２は攻撃の可能性ある怪しいグループのパケットを受け取るサーバであるが、何れも同一のサービス提供機能をもつものであり、異なる機器どうしの場合には冗長構成のとれる機器どうしの組み合わせが好ましい。なお、防御対象の主系２１と従系２２は、１対１の関係にあるが、１つの主系２１に対して複数の従系２２，…、又は主系２１と従系２２がそれぞれ複数存在する構成であってもよい。

【００２６】

パケット転送装置３０は、パケット送信元１１から防御対象にアクセスしようとするパケットを受信するネットワークインタフェース３１、このインタフェース３１により受信されたパケットから未知の攻撃の可能性有無を判定する未知攻撃判定部３２、防御対象におけるネットワークの冗長構成を規定するアノーマリ型パケット転送テーブル３３、この未知攻撃判定部３２による判定結果に基づき、パケット転送テーブル３３の冗長構成を参照し、パケットの振分け処理を実行するパケット振分け部３４及び振分け処理結果に従って受信パケットを主系２１ａ、従系２１ｂの何れかに転送するネットワークインタフェース３５が設けられている。

【００２７】

未知攻撃判定部３２は、パケット解析部３２１、パケット統計解析テーブル３２２及びア

ノーマリ評価部３２３によって構成されている。パケット解析部３２１及びパケット統計解析テーブル３２２は、複数のパケットから構成されるアプリケーションデータを解析し記憶する機能をもつものであり、具体的には、パケット解析部３２１が複数のパケットを採取し、防御対象で使用されるプロトコルレイヤのアプリケーションデータ（分割された複数のパケットの組み合わせデータ）を構成し、当該プロトコルレイヤによって規定される規則を利用し、文字区分や数値情報等を抽出し解析することにより、図２に示すような統計的な評価値ｆ（ｘ）を算出し、この評価値ｆ（ｘ）から例えば平均値や分散を計算し、後記する図４に示すごとく統計情報としてパケット統計解析テーブル３２２に記憶する。

【００２８】

前記アノーマリ評価部３２３は、パケット統計解析テーブル３２２に記憶されたアプリケーションデータの解析結果である統計情報から統計的に正常な値域ｙ１、統計的に異常な値域ｙ２を評価し、正常な値域ｙ１及び異常な値域ｙ２に属する評価結果をパケット振分け部３４に送出する。なお、図示されていないが極めて異常な値域に属するの場合は、パケット解析部３２１又はアノーマリ評価部３２３でパケットが捨てられ、防御対象へのアクセスを遮断する。

【００２９】

パケット振分け部３４は、アノーマリ評価部３２３からの評価結果に基づき、統計的に正常な値域ｙ１に属するパケットの場合、アノーマリ型パケット転送テーブル３３の冗長構成に基づき、受信パケットを主系２１に振分け、統計的に異常な値域ｙ２に属するパケットの場合、同様の手順に基づいて従系２２に受信パケットを振分ける処理を実行する。ネットワークインタフェース３５は、振分け処理結果に従って主系２１又は従系２２の何れかに受信パケットを転送する。

【００３０】

なお、パケット統計解析テーブル３２２とアノーマリ型パケット転送テーブル３３はそれぞれ個別のテーブルが使用されているが、後記する図５に示すように同一のテーブルを区分けして使用してもよい。

【００３１】

次に、本発明の第１の実施の形態に係わるプログラム及びパケット転送方法について図３及び図４を参照しながら説明する。図３はパケット転送装置３０がＣＰＵで構成されている場合、このパケット転送装置３０には受信パケットを防御対象の主系２１と従系２２とに振分け処理するプログラムを格納するプログラムメモリ４１が接続される。

【００３２】

先ず、パケット転送装置３０が動作を開始すると、プログラムメモリ４１に格納されるプログラムを読み出し、適宜なメモリに格納する。この状態において、パケット送信元１１から第１のネットワーク１０を通じて防御対象にアクセスしようとするパケットが到来すると、当該パケットをネットワークインタフェース３１にて受信し、パケット解析部３２１に相当するパケット解析機能３２１ａに渡す（Ｓ１：パケット受信ステップ）。

【００３３】

このパケット解析機能３２１ａは、受信したパケットに関し、前述するように防御対象２１で使用されるプロトコルレイヤのアプリケーションデータを構成し、このアプリケーションデータから文字区分や数値情報等を抽出し解析し（Ｓ２）、統計的な評価値ｆ（ｘ）を算出し、この評価値ｆ（ｘ）から平均値や分散を求め、統計情報としてパケット統計解析テーブル３２２に記憶する（Ｓ３）。このＳ２，Ｓ３はパケット解析ステップに相当する。

【００３４】

引き続き、パケット転送装置３０は、アノーマリ評価部３２ｃに相当するアノーマリ評価機能３２３ａを実行する。このアノーマリ評価機能３２３ａは、パケット統計解析テーブル３２２に記憶された統計情報から統計的に正常な値域ｙ１か統計的に異常な値域ｙ２か、つまり統計的に「アリーマリ」であるか否かを判断する（Ｓ４：アリーマリ評価ステッ

プ）。ここで、「アリーマリ」とは、過去に防御対象２１にアクセスしたパケットの解析結果（統計情報）を参照し、統計的に異常であると評価されるものを指す。このようなパケットは、完全に攻撃とは言い切れないが、攻撃の可能性があると判断される。

【００３５】

さらに、パケット転送装置３０は、パケット振分け部３４に相当する転送先決定機能３４ａを実行する。この転送先決定機能３４ａは、パケットが「アリーマリ」であると評価された場合、パケット転送テーブル３３の冗長構成を参照し、パケットの転送先を防御対象の従系２２であると決定し（Ｓ５）、またパケットが「アリーマリ」でないと評価された場合、同じくパケット転送テーブル３３の冗長構成からパケットの転送先を防御対象の主系２１であると決定する（Ｓ６：パケット振分けステップ）。

【００３６】

さらに、パケット転送機能３５ａを実行する。このパケット転送機能３５ａは、ステップＳ５によるパケット転送先決定に基づいて受信パケットを防御対象の従系２２に転送し（Ｓ７）、またＳ６によるパケット転送先決定に基づいて受信パケットを防御対象の従系２１に転送する（Ｓ８）。このＳ７，Ｓ８はパケット転送ステップに相当する。

【００３７】

従って、以上のような実施の形態であるパケット転送システム、パケット転送装置、プログラム及びパケット転送方法によれば、未知の攻撃の可能性があると評価した場合には、防御対象の従系２２に転送するが、この従系２２は、未知の攻撃の可能性のある怪しいパケットを受けもつサーバであるが、主系２１とほぼ同様のサービス機能を有するので、仮にパケットが攻撃無しであれば、主系２１とほぼ同様のサービス機能を提供することができる。一方、従系２２が受け取ったパケットが真に攻撃的なパケットであれば、直接の被害を受けるが、その被害は従系２２であり、主系２１は直接の被害を受けなくなるから、未知の攻撃に対して、防御対象の可用性が高くなる効果を期待できる。

【００３８】

また、「アリーマリ」と評価されたパケットは、攻撃ではないが、通常のサービスを要求しない可能性もある。例えば攻撃者が攻撃を行う前に、正常な使われ方でないパケットを防御対象に送り付け、当該防御対象からの応答パケットを調べて攻撃の手口を探るフィンガープリンティングという手法を利用する例もある。このような手法を利用したパケットを防御対象の主系２１に転送した場合、主系２１はそのパケット処理が無駄となり、防御対象本来のサービス提供に振り向けられず、処理能力の低下となる。しかし、本発明においては、「アリーマリ」でないと評価されるパケットが従系２２に転送するので、主系２１による無駄処理がなくなり、迅速にサービスを提供することができる。

【００３９】

なお、前記未知攻撃判定部３２は、様々なプロトコルレイヤを対象とするので、それぞれ防御対象により使用されるプロトコルレイヤに規定されるデータフォーマットに応じた統計解析処理が実施できるようにすることが好ましい。

【００４０】

次に、具体的にＷｅｂサーバを用いた防御対象に対する未知の攻撃の判断の一例について説明する。

【００４１】

このＷｅｂサーバに対する攻撃の典型的な事例としては、ＣＧＩ（Ｃｏｍｍｏｎ　Ｇａｔｅｗａｙ　Ｉｎｔｅｒｆａｃｅ）に特別なメタキャラクタを伴うスクリプトが挿され、Ｗｅｂサーバが実行されてしまったり、或いは特別に長い文字列を与えることによりＣＧＩにバグを発生させ、Ｗｅｂサーバにバッファオーバーフローなどの誤動作を起こさせるなど、攻撃として成立する事例が非常に多く出回っている。また、攻撃が成立した場合、通常人間がＷｅｂブラウザから入力しないような長いバイナリコードをＷｅｂサーバに送り付け、実行させられる例もある。さらに、インターネット上で取り扱うＣＧＩは、日々新たに開発されており、それに伴って未知の脆弱性と未知の攻撃も増え続けている。

【００４２】

そこで、Ｗｅｂサーバに対する未知の攻撃の可能性を判定する場合においては、ＣＧＩに与える変数の値を構成する文字セットを分類分けし、各文字セットごとに統計的な分布から「アノーマリ」を評価することが好ましい。

【００４３】

以下、各文字セットごとに統計的な分布から「アノーマリ」を評価する例について説明する。

【００４４】

未知攻撃判定部３２のパケット解析部３２１は、パケット送信元１１から防御対象にアクセスするパケットを採取し、複数のパケットのデータからアプリケーションデータを構成する。このアプリケーションデータは、防御対象がＷｅｂサーバであるので、ＨＴＴＰ（Ｈｙｐｅｒｔｅｘｔ Ｔｒａｎｓｆｅｒ Ｐｒｏｔｏｃｏｌ）データを構成する。パケット解析部３２１は、アプリケーションデータであるＨＴＴＰデータを、ＨＴＴＰで規定されるプロトコルに従って解釈し、ＵＲＬ名，ＣＧＩの変数名，変数の値，この値に含まれる文字等の文字列区分や数値情報を抽出し、統計的な評価分布から平均値，分散を取得し、パケット統計解析テーブル３２２に記憶する。

【００４５】

図５はＷｅｂサーバにアクセスするパケットに関するパケット統計解析テーブル３２２とアノーマリ型パケット転送テーブル３３のデータ配列例を示す図である。パケット統計解析テーブル３２２は、Ｗｅｂサーバにアクセスするアプリケーションデータを解析し、かつ、統計的に解析した統計情報が記憶される。このテーブルの行５１は、ＵＲＬ名を記憶するエリアであり、例えばＵＲＬ名ａ，ＵＲＬ名ｂ，ＵＲＬ名ｃ，…のように記憶する。一方、テーブルの列５２は、ＵＲＬで示されるものがＣＧＩである場合、ＣＧＩに与えられた変数名を記憶するエリアであり、例えば変数名ｘ１，変数名ｘ２，変数名ｘ３，…のように記憶する。但し、Ｗｅｂサーバにアクセスするデータの中には全く変数が与えられないＵＲＬもある。

【００４６】

一般に、ＵＲＬ名と変数名は、Ｗｅｂサーバ内では限られた数であるので、防御対象であるＷｅｂサーバにアクセスしてくるＨＴＴＰデータから学習記憶し、テーブルの行・列に順次記憶しておく。

【００４７】

ＵＲＬ名と変数名から参照される個々のセルは、詳しくは統計情報を記憶されるセル５３であって、学習段階において蓄積される統計情報が記憶される。つまり、あるＵＲＬ名ｂに与えられたある変数名ｘ２に関する値の統計情報が記憶される。このセル５３の行５４は、値の構成要素を分類分けするものであり、文字セットＡ，文字セットＢ，文字セットＣ，…のように分類分けする。この文字セットＡ，Ｂ，…は、具体的には「数値」，「ＡＳＣ１１（アスキー）文字」，「メタキャラクタ（プロトコルやスクリプト言語で特殊な意味をもつ文字）」，「その他（例えばバイナリコード）」などに分類される。このセル５３の列５５は、値の長さに関する統計情報を記憶するものであって、ＨＴＴＰがアクセルされる毎に学習段階で図２に示す統計的な評価分布に基づいて平均値５６，分散５７を再計算し、当該再計算の度に更新される。

【００４８】

以上のようにして充分に学習された統計情報に基づき、次のようなアリーマリ評価を実施する。すなわち、パケット送信元１１から防御対象をアクセスするためにＨＴＴＰデータが与えられた場合、このＨＴＴＰデータのもとにパケット統計解析テーブル３２２に該当するＵＲＬ名と変数名との組が存在するか否かを判断し、存在する場合にはそのセル５３内に記憶される統計情報を参照し、値の構成要素である文字セットの各々について、値の長さの平均値５６と分散５７とに基づいて統計的に異常な値域であるかどうか、すなわちアノーマリであるか否かを判定する。この判定処理は、アノーマリ評価関数ｆ（ｘ１，ｘ２，ｘ３，…）による値の計算と形式的に同一視できる。

【００４９】

そして、評価値が正常値の値域に属するならば防御対象の主系２１にパケットを転送し、評価値が異常値の値域に属するならば防御対象の従系２２２にパケットを転送する。ところで、アノーマリ評価関数ｆ（ｘ１，ｘ２，ｘ３，…）による値域からパケットの転送先を決定するが、この決定に際しては、予めＵＲＬ毎に、アノーマリ評価関数ｆ（ｘ１，ｘ２，ｘ３，…）による値域と、それに対するパケット転送先とを規定するアノーマリ型パケット転送テーブル３３を参照し、主系２１か従系２２かを決定する。

【００５０】

なお、パケット送信元１１から与えられるパケットのＨＴＴＰデータが一度もアクセスされたことのないＵＲＬ名と変数名との組、或いは単にＵＲＬ名だけの場合、その時点でアノーマリと判定してもよい。また、ＷｅｂサーバのＣＧＩによっては、変数名が与えられず値のみが与えられる。このような場合には、パケット統計解析テーブル３２２は、変数名を考慮した二次元の「表形式」である必要はなく、ＵＲＬ名だけの一次元の「列」で構成されることもある。

【００５１】

また、以上の実施の形態では、防御対象が主系２１と従系２２からなる二重構成であるが、それ以上の多重構成であってもよい。この場合には、アノーマリ型パケット転送テーブル３３のアノーマリ評価関数ｆ（ｘ１，ｘ２，ｘ３，…）の値域を複数設定し、それに対応したパケット転送先を複数設定することになる。

【００５２】

（第２の実施の形態）

図６は本発明に係るパケット転送システムの一実施の形態を示す系統構成図である。なお、このパケット転送システムは、その大部分が図１とほぼ同様な構成であるので、同一部分には同一符号を付し、詳しくは図１及びその関連図の説明に譲る。

【００５３】

このパケット転送システムの特に異なるところは、防御対象、パケット転送装置３０の一部の構成であるアノーマリ型パケット転送テーブル３３及びネットワークインタフェース３５を含むパケット振分け部３４を改良した点にある。

【００５４】

防御対象は、複数の従系２２１，…，２２Ｎが設置され、主系２１を含むこれら各従系２２１，…，２２Ｎにはそれぞれホスト型ＩＤＳ２３、２４１，…，２４Ｎが設けられている。ここで、ホスト型ＩＤＳとは、防御対象のホスト上に適用される実際の攻撃を検知する機能をもったプログラムである。

【００５５】

なお、アノーマリ評価関数ｆ（ｘ１，ｘ２，ｘ３，…）の値域としては、図７に示すように統計的に正常な値域ｙ１と、統計的に異常な値域ｙ２と、統計的に特に異常な値域ｙ３とがあるが、そのうち統計的に特に異常な値域ｙ３は、通常，パケット解析部３２１又はパケット振分け部３４で遮断されるが、統計的に異常な値域ｙ２については、前述する複数の従系２２１，…，２２Ｎを設けることにより、アノーマリ型パケット転送テーブル３３は、例えば図８（ａ）～（ｃ）に示すようにアノーマリ評価関数ｆ（ｘ１，ｘ２，ｘ３，…）の値域とパケットの転送先とを関係付ける構成を採用する。

【００５６】

同図（ａ）は、アノーマリ評価関数ｆ（ｘ１，ｘ２，ｘ３，…）の値域ｙ１，ｙ２，ｙ３，…のうち、値域ｙ２に対して防御対象の複数の従系２２１，…，２２Ｎを割当てる例である。同図（ｂ）は、アノーマリ評価関数ｆ（ｘ１，ｘ２，ｘ３，…）の値域ｙ１，ｙ３に対してパケット転送先を共通に設定し、アノーマリ評価関数ｆ（ｘ１，ｘ２，ｘ３，…）の値域ｙ２については各変数名ごとに防御対象の従系２２１，…，２２Ｎを割当てる例である。また、同図（ｃ）は、統計的に異常な値域ｙ２を複数の値域ｙ２１，…，ｙ２ｎに分け、これら値域ｙ２１，…，ｙ２ｎごとに従系２２１，…，２２Ｎを割当てる例である。

【００５７】

すなわち、未知攻撃判定部３２は、図８（ａ）に示すアノーマリ型パケット転送テーブル３３を用いる場合、未知攻撃の可能性ありと評価されたとき、通常，パケット振分け部３４が従系２２１を転送先と決定し、パケットを転送するが、当該従系２２１に対応するホスト型ＩＤＳ２４１で本当の攻撃と検知された場合、次に受信されるパケットに対して次の従系２２２（図示せず）を転送先と決定する。これは従系２２１を復旧させる間でも、引き続き、他の防御対象の従系２２２がサービスを提供可能な状態にするためである。また、未知攻撃判定部３２は、図８（ｂ）、（ｃ）に示すアノーマリ型パケット転送テーブル３３を用いる場合、パケット振分け部３４で決定されるパケット転送先に従ってパケットを転送する。図８（ｂ）の場合には、何れかの変数名で攻撃可能性を判定した場合、当該変数名から従系を決定する。図８（ｃ）の場合には、何れの値域ｙ２１，…，ｙ２ｎで攻撃可能性を判定した場合、ひいては該当値域に基づいて従系をパケット転送先と決定する。

【００５８】

従って、図８（ａ）～（ｃ）のようなアノーマリ型パケット転送テーブル３３を構成することにより、より正しい評価を下すことが可能であり、攻撃があった場合にもサービスの継続性を維持することが可能である。

【００５９】

次に、本発明における第２の実施の形態に係わるプログラム及びパケット転送方法について図９及び図１０を参照しながら説明する。但し、この例は、図８（ａ）に示すアノーマリ型パケット転送テーブル３３を用いた例について説明する。

【００６０】

パケット転送装置３０がＣＰＵで構成されている場合、このパケット転送装置３０には受信パケットを防御対象の主系２１と従系２２１，…，２２Ｎとに振分け処理するプログラムを格納するプログラムメモリ５８が設けられている。

【００６１】

先ず、パケット転送装置３０が動作を開始すると、プログラムメモリ５８に格納されるプログラムを読み出し、プログラムを実行するが、機能的にはパケット解析機能３２１ａ、アノーマリ評価機能３２３ａ、転送先決定機能３４ａ、パケット転送機能３５ａは図３と同様であり、またパケット転送処理手順については、図４の処理手順Ｓ１～Ｓ７と同様であるので、それぞれの図の説明に譲り、以下，異なる部分について説明する。

【００６２】

すなわち、パケット転送装置３０は、パケット転送機能３５ａによってパケットを転送した後（Ｓ７）、従系攻撃検知識別機能３４ｂを実行する。この従系攻撃検知識別機能３４ｂは、パケットを転送した後、転送先の従系例えば２２１に対応するホスト型ＩＤＳ２４１が攻撃を検知したか否かを判断する（Ｓ１１）。このホスト型ＩＤＳ２４１は、ネットワークインタフェース３５からパケットを受け取ると、前述するように実際の攻撃であるか否かを検知し、攻撃であると検知するとトリガ情報として例えばＳＮＭＰ（Ｓｉｍｐｌｅ　Ｎｅｔｗｏｒｋ　Ｍａｎａｇｅｍｅｎｔ　Ｐｒｏｔｏｃｏｌ）トラップをパケット転送装置３０に通知する。従って、従系攻撃検知識別機能３４ｂは、転送先である従系２２１から攻撃検知の通知を受けると、何れの防御対象上で攻撃を検知したかを識別する（Ｓ１２）。このＳ１１，Ｓ１２は従系攻撃検知識別ステップに相当する。

【００６３】

引き続き、パケット転送装置３０は従系切替機能３５ｂを実行する。この従系切替機能３５ｂは、アノーマリ型パケット転送テーブル３３に規定する図８（ａ）から予め定められた順序に従つて例えば従系２２２に切り替え、以降に受信する攻撃可能性あるパケットを転送する（Ｓ１３：従系切替ステップ）。

【００６４】

なお、アノーマリ型パケット転送テーブル３３の構成が図８（ｂ）、（ｃ）の場合、パケット振分け部３４又は転送先決定機能３４ａは、アノーマリ型パケット転送テーブル３３に規定する冗長構成から、統計的に異常な複数レベルの値域ｙ２１，ｙ２２，…または変

数名に基づいて決定し、ホスト型ＩＤＳをもつ複数の従系２２１，…，２２Ｎの中から１の従系を振分け先とする。

【００６５】

従って、以上のような第２の実施の形態によれば、少なくとも防御対象にホスト型ＩＤＳをもつ複数の従系２２１，…，２２Ｎを設け、パケット転送装置３０は、受信パケットが攻撃可能性有りと評価されたとき、アノーマリ型パケット転送テーブル３３の規定に従って１つの従系にパケットを転送するが、この転送先従系のホスト型ＩＤＳから攻撃検知の通知を受けたとき、予め定める次の従系にパケットを転送するように切替えるので、当該攻撃を受けた従系を復旧させる間にパケットを受信しても、他の従系に振り分けてサービスを提供することが可能となり、防御対象の可用性を高めることができる。

【００６６】

なお、上記実施の形態は、従系のホスト型ＩＤＳから攻撃検知の通知を受けたとき、パケット転送テーブル３３の規定に従って次の従系に切替える構成であるが、例えば従系のホスト型ＩＤＳから攻撃検知の通知を受けたとき、攻撃検知時のアプリケーションデータをアノーマリ評価関数により再評価し、その評価値を閾値とし、統計的に特に異常な値域ｙ３に属させ、パケットを明示的に遮断する学習ルールとしてもよい。すなわち、図７に示すように、アプリケーションデータの解析による統計的な評価値ｆ（ｘ）に対し、統計的に正常な値域ｙ１と、統計的に異常な値域ｙ２と、従系側のホスト型ＩＤＳで攻撃検知とされたデータの評価値を閾値とする統計的に特に異常な値域ｙ３に属させ、攻撃の可能性が高く、かつ、統計的に特に異常な値域に属する場合には明示的にパケットを遮断すれば、攻撃の可能性が高いものに対する防御対象の安全性を向上させることができる。

【００６７】

（第３の実施の形態）

図１１は本発明に係るパケット転送システムの一実施の形態を示す系統構成図である。

【００６８】

このパケット転送システムは、パケット送信元１１が設けられている第１のネットワーク１０と、冗長構成化された主系と１つ又は複数の従系とを備えた防御対象が設けられている第２のネットワーク２０と、これらネットワーク１０，２０を行き来するパケットを転送するパケット転送装置とが設けられている点は第１、第２の実施の形態と同様である。従って、第２のネットワーク２０に設けられる防御対象は、第１、第２の実施の形態と同様な構成であるので、それらの説明に譲り、その具体的な構成は図面から省略している。

【００６９】

この実施の形態において、特に異なるところは多重化されたパケット転送装置３０Ａ，３０Ｂを設けたこと、また複数のパケット転送装置３０Ａ，３０Ｂとネットワーク２０との間にＵＲＬスイッチ６０を設置する一方、当該ＵＲＬスイッチ６０とネットワーク２０間に複数のパケット転送装置３０Ａ，３０Ｂを介さずに直接接続される伝送ライン６１を設けたことなどである。なお、パケット転送装置３０Ａ，３０Ｂの構成は、第１、第２の実施の形態と同様な構成であるので、それらの実施の形態の説明に譲り、図面にはパケット統計解析テーブル３２２Ａ，３２２Ｂだけを記載し、他の具体的な構成は省略する。

【００７０】

以上のようにパケット転送装置を多重化構成とした理由は次の通りである。パケット転送装置は、統計解析を行う観点から、アプリケーションデータのＵＲＬ名のみならず、ＣＧＩの変数名、各変数名の値などが必要となり、防御対象のトラフィック量が大きくなり、スループットが十分に出なくなる懸念がある。

【００７１】

そこで、この実施の形態では、複数のパケット転送装置３０Ａ，３０Ｂを設け、パケット転送装置３０Ａには図１２（ｂ）に示すパケット統計解析テーブル３２２Ａ、パケット転送装置３０Ｂには図１２（ｃ）に示すパケット統計解析テーブル３２２Ｂを設けるとともに、複数のパケット転送装置３０Ａ，３０Ｂとネットワーク１０との間にＵＲＬスイッチ６０を設け、負荷の分散を図る構成を採用している。

【００７２】
このＵＲＬスイッチ６０は、レイヤ７スイッチとも言われ、一種の負荷分散装置であり、図１２（ａ）に示すように負荷分散テーブル６２にＵＲＬと負荷分散先とを関係付け、パケットの分散を図る構成である。ＵＲＬスイッチ６０は、例えば専用のハードウエア構成によりアプリケーションデータに含まれるＵＲＬを高速に解読し、この解読されたＵＲＬのもとに負荷分散テーブル６２を参照し、複数のパケット転送装置３０Ａ，３０Ｂ、ネットワーク２０のいずれかにパケットを振分ける。
【００７３】
さらに、図１１に示すパケット転送システムについて詳細に説明する。
【００７４】
第１の実施の形態における図５に示すパケット統計解析テーブル３２２に着目すると、ＵＲＬ名が当該テーブルの行に一意に記憶されている。一方、この実施の形態では、図１２に示すようにＵＲＬ名に基づいてテーブルを複数に分割し、この分割されたテーブル数だけパケット転送装置を設置し、分割されたテーブルを各パケット転送装置に個別に割り当てている。
【００７５】
一方、ＵＲＬスイッチ６０における負荷分散テーブル６２にはＵＲＬ名と負荷分散先とを関係付けることにより、アプリケーションデータに含まれるＵＲＬに基づき、負荷分散テーブル６２から分散先である１つのパケット転送装置を検索し、アプリケーションデータの統計解析処理を実行させることにより、防御対象のＵＲＬ名の数と、防御対象に対するトラフィック量とが大きくなっても、スループットの低下を抑えるようにする。
【００７６】
ところで、多数のＵＲＬのうち、特定のＵＲＬ（例えばＵＲＬ名ｇ，ＵＲＬ名ｈ，ＵＲＬ名ｉ）は、パケット転送装置による統計解析によって変数が全く与えられないことが明らかな場合、当該ＵＲＬ名を含むアプリケーションデータは、ＵＲＬスイッチ６０からパケット転送装置を経由させずに直接に防御対象が存在するネットワーク２０に向けるように、負荷分散テーブル６２を変更することが好ましい。
【００７７】
そこで、パケット転送装置は、統計的に変数が全く与えられないＵＲＬのリストをＵＲＬスイッチ６０に通知し、当該ＵＲＬ名とともにパケット分散先をネットワーク２０の防御対象であることを負荷分散テーブル６２に登録する。なお、ＵＲＬのリストを通知するためのプロトコル手段は、ＵＲＬスイッチ６０が解釈できるものであれば特に問わない。これにより、変数名やその値に関する攻撃の可能性の無いパケットは、アプリケーションデータの統計解析処理と異常性の評価処理が省略されるので、スループットの低下を抑制する効果が得られる。
【００７８】
また、パケット転送装置は、統計解析により、与えられる変数の数が比較的多いことが明らかになった場合、同様にＵＲＬスイッチ６０に通知する。その結果、ＵＲＬスイッチ６０は、以上のようなＵＲＬ名を含むアプリケーションデータを比較的処理性能の高いパケット転送装置に向けるように負荷分散テーブル６２に登録する。これにより、変数の数が比較的多く、統計解析処理と異常性の評価処理の負荷が大きいアプリケーションデータは、処理性能の高いパケット転送装置に処理させる。一方、変数の数が比較的少なく、統計解析処理と異常性の評価処理の負荷が小さいアプリケーションデータは、処理性能の低いパケット転送装置に処理させることにより、全体的にバランスよく負荷を分散でき、スループットの低下を抑制できる効果を奏する。
【００７９】
なお、本願発明は、上記実施の形態に限定されるものでなく、その要旨を逸脱しない範囲で種々変形して実施できる。上記実施の形態における未知攻撃の判定は、ＨＴＴＰに限らず、インタネットの様々な通信プロトコルでも同様に適用できる。インターネットにおける通信プロトコルは、予め規定される予約語によって識別されるＴＬＶ（Ｔｙｐｅ　Ｌｅ

ｎｇｔｈ　Ｖａｌｕｅ）と、その値との組み合わせにより表現され、プロトコルサーバに送信する例が多い。これは、Ｗｅｂサーバにおいて取り扱うＣＧＩに類似し、プロトコルサーバへの攻撃手法も、Ｗｅｂサーバへの攻撃手法と類似するので、前述する実施の形態と同様に未知攻撃の可能性を判定する。

【００８０】

具体的には、電子メールの送信や中継を行うＳＭＴＰ（Ｓｉｍｐｌｅ　Ｍａｉｌ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ）やＦＴＰでは、「コマンド」として規定されているＴＬＶの変数の値が長い値で与えられた場合、ＳＭＴＰサーバやＦＴＰサーバがバッファオーバフローしてしまう攻撃が数多く存在する。また、ＤＮＳ（Ｄｏｍａｉｎ　Ｎａｍｅ　Ｓｙｓｔｅｍ）において「クエリ」と規定されているＴＬＶについても同様である。

【００８１】

さらに、ＢＧＰ（Ｂｏｒｄｅｒ　Ｇａｔｅｗａｙ　Ｐｒｏｔｏｃｏｌ）やＯＳＰＦ（Ｏｐｅｎ　ＳｈｏｒｔｅｓｔＰａｔｈ　Ｆｉｒｓｔ）といったルーティングプロトコルの分野では、ベンダー（Ｖｅｎｄｅｒ）が製品開発のために自由に定義できるＴＬＶを許している例が多い。このことは、ベンダーが未定義のＴＬＶに値を入れるだけで、当該ベンダーのプロトコルサーバがクラッシュしてしまう攻撃も存在する。よって、ＴＬＶ形式を用いたアプリケーションのプロトコルサーバに対する未知攻撃を判定するために、上記実施の形態で説明したＷｅｂサーバを対象とした場合の未知攻撃判定方法を適用すれば、有効な解決手段となりうるものである。

【００８２】

また、各実施の形態は可能な限り組み合わせて実施することが可能であり、その場合には組み合わせによる効果が得られる。さらに、上記各実施の形態には種々の上位，下位段階の発明が含まれており、開示された複数の構成要素の適宜な組み合わせにより種々の発明が抽出され得るものである。例えば問題点を解決するための手段に記載される全構成要件から幾つかの構成要件が省略されうることで発明が抽出された場合には、その抽出された発明を実施する場合には省略部分が周知慣用技術で適宜補われるものである。

【００８３】

【発明の効果】

以上説明したように本発明によれば、未知の攻撃に対し、攻撃検知の正確性が完全でない場合でも、防御対象の正常なサービスを停止させず、当該防御対象の致命的な被害から守ることができるパケット転送システム、パケット転送装置、プログラム及びパケット転送方法を提供できる。

【図面の簡単な説明】

【図１】本発明の第１の実施の形態に係るパケット転送システム及びパケット転送装置を示す構成図。

【図２】図１に示すパケット転送装置によって複数の受信パケットから得られる通信アプリケーションデータの解析による統計的な評価値を説明する分布図。

【図３】本発明の第１の実施の形態に係るプログラム及びパケット転送方法を説明する機能ブロック図。

【図４】本発明の第１の実施の形態に係るプログラム及びパケット転送方法を説明する処理の流れ図。

【図５】パケット統計解析テーブル及びアノーマリ型パケット転送テーブルのデータ配列図。

【図６】本発明の第２の実施の形態に係るパケット転送システム及びパケット転送装置を示す構成図。

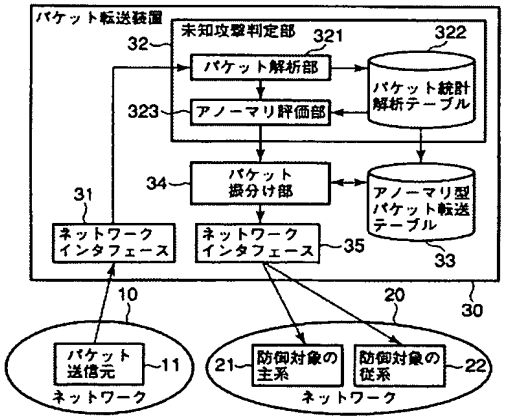
【図７】図６に示すパケット転送装置によって複数の受信パケットから得られる通信アプリケーションデータの解析による統計的な評価値を説明する分布図。

【図８】アノーマリ型パケット転送テーブルのデータ配列図。

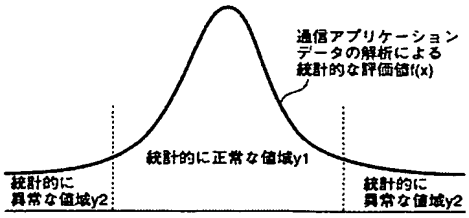
【図９】本発明の第２実施の形態に係るプログラム及びパケット転送方法を説明する機能ブロック図。

【図１０】本発明の第２の実施の形態に係るプログラム及びパケット転送方法を説明する処理の流れ図。
【図１１】本発明の第３の実施の形態に係るパケット転送システムを示す構成図。
【図１２】ＵＲＬスイッチの負荷分散テーブルによる負荷の分散状態を説明する図。
【図１３】従来の通信アプリケーションデータの解析による統計的な評価値を説明する分布図。
【符号の説明】
１０…第１のネットワーク、１１…パケット送信元、２０…第２のネットワーク、２１…防御対象の主系、２２，２２１～２２Ｎ…防御対象の従系、３２…未知攻撃判定部、３３…アノーマリ型パケット転送テーブル、３４…パケット振分け部、３４ａ…転送先決定機能、３４ｂ…従系攻撃検知識別機能、３２１…パケット解析部、３２１ａ…パケット解析機能、３２２…パケット統計解析テーブル、３２３…アノーマリ評価部、３２３ａ…アノーマリ評価機能、２３，２４１～２４Ｎ…ホスト型ＩＤＳ、３５ａ…パケット転送機能、３５ｂ…従系切替機能。

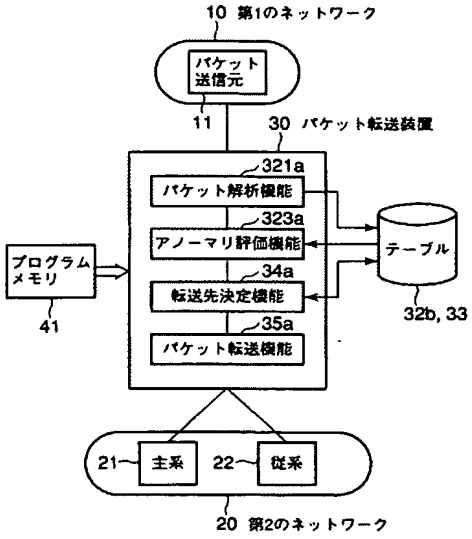
【図１】



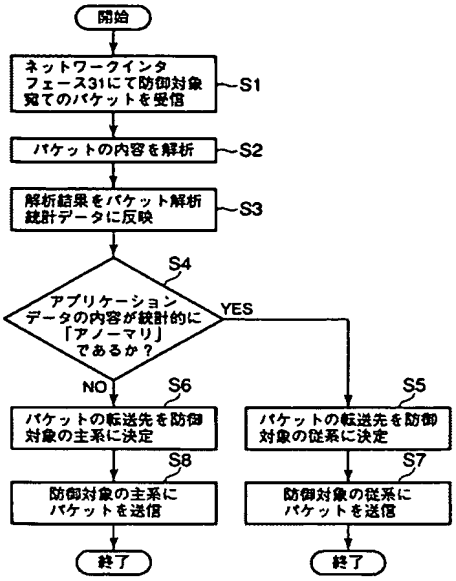
【図２】



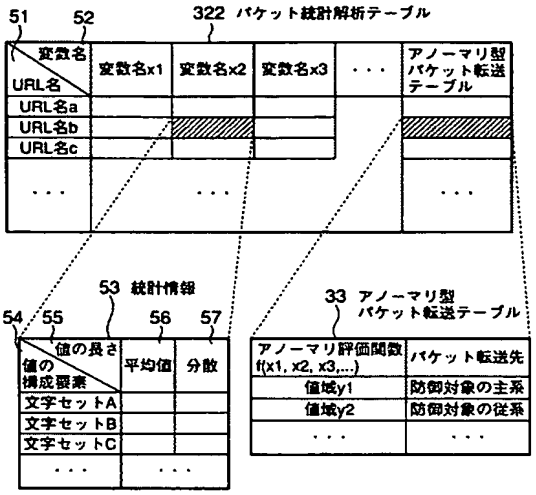
【図３】



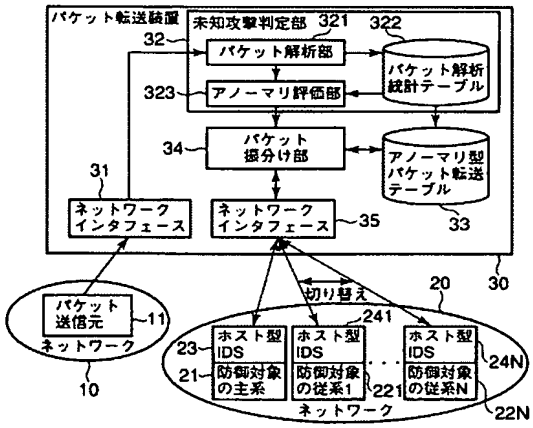
【図４】



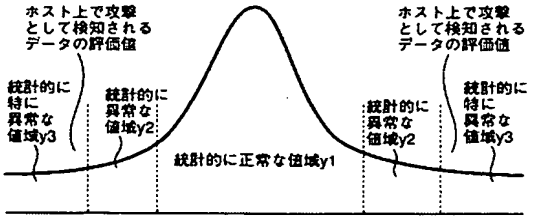
【図５】



【図６】



【図７】



【図８】

(a)

33

アノーマリ評価関数 f(x1, x2, x3,...)	パケット転送先
値域y1	防御対象の主系
値域y2	防御対象の従系
値域y3	遮断
...	...

従系1
従系2
従系3
...
従系N

(b)

33

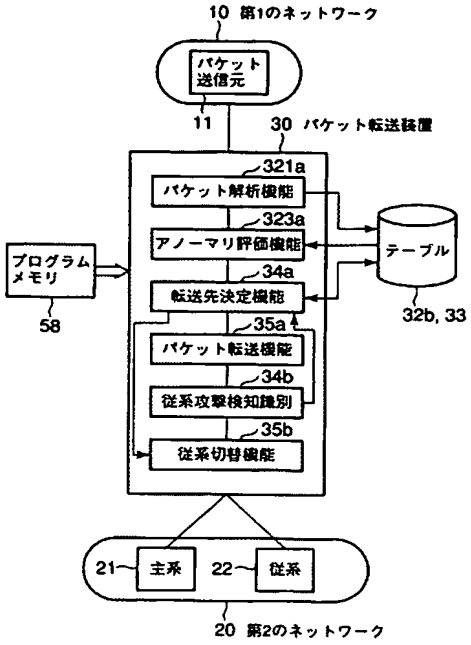
変数名	アノーマリ評価関数	パケット転送先
x1, x2,...	y1	主系
	y3	遮断
x1	y2	従系1
x2	y2	従系2
x3	y2	従系3
...	...	...

(c)

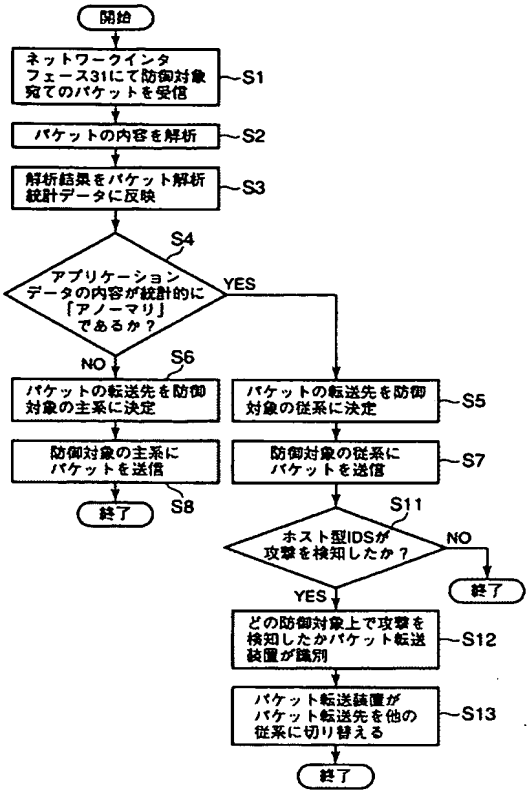
33

アノーマリ評価関数	パケット転送先
y1	主系
y21	従系1
y22	従系2
y23	従系3
...	...
y3	遮断

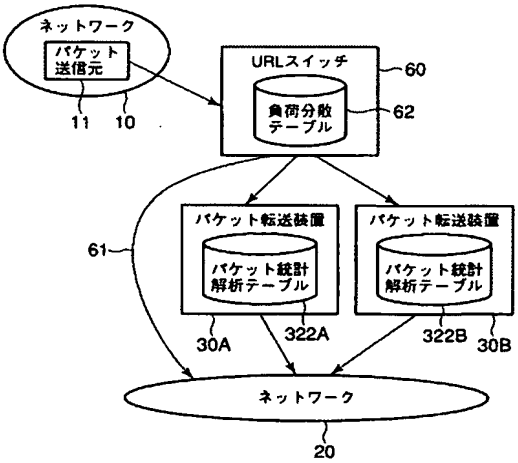
【図９】



【図１０】



【図１１】



【図１２】

(a)

URLスイッチの負荷分散テーブル

	URL名	負荷分散先
パケット転送装置30Aへ	URL名a	30A
	URL名b	30A
	URL名c	30A
パケット転送装置30Bへ	URL名d	30B
	URL名e	30B
	URL名f	30B
ネットワーク20へ	URL名g	20
	URL名h	20
	URL名i	20
	・・・	・・・

(b)

322A

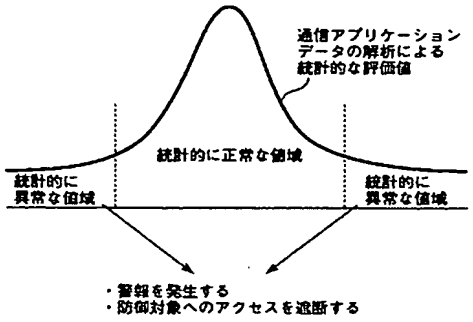
変数名 / URL名	変数名x1	変数名x2	変数名x3	・・・	アノーマリ型パケット転送テーブル
URL名a					
URL名b					
URL名c					
・・・	・・・	・・・	・・・	・・・	・・・・・・

(c)

322B

変数名 / URL名	変数名x1	変数名x2	変数名x3	・・・	アノーマリ型パケット転送テーブル
URL名d					
URL名e					
URL名f					
・・・	・・・	・・・	・・・	・・・	・・・・・・

【図１３】


通信アプリケーション
データの解析による
統計的な評価値
統計的に正常な領域
統計的に
異常な領域
統計的に
異常な領域
・警報を発生する
・防御対象へのアクセスを遮断する

フロントページの続き

(72)発明者 今野 徹
東京都府中市東芝町１番地 株式会社東芝府中事業所内

Ｆターム(参考) 5K030 GA15 HB16 HD06 KA07 LB08
5K033 AA08 CB08 DA06 DB18